PCT/JP99/02510

17.06.99

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１０月２８日

出 願 番 号
Application Number: 平成１０年特許願第３０７６５８号

出 願 人
Applicant (s): 三菱マテリアル株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

１９９９年 ４月 ９日

特 許 庁 長 官
Commissioner,
Patent Office

出証番号 出証特平１１－３０２１０９０

【書類名】　特許願

【整理番号】　J75325A1

【提出日】　平成10年10月28日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C　1/00

【発明の名称】　暗号化装置、復号化装置、方法及びその記録媒体

【請求項の数】　10

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社　総合研究所内

【氏名】　大久保　達真

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社　総合研究所内

【氏名】　佐分利　徹

【特許出願人】

【識別番号】　000006264

【氏名又は名称】　三菱マテリアル株式会社

【代理人】

【識別番号】　100064908

【弁理士】

【氏名又は名称】　志賀　正武

【選任した代理人】

【識別番号】　100108578

【弁理士】

【氏名又は名称】　高橋　詔男

【選任した代理人】

【識別番号】　100089037

【弁理士】

【氏名又は名称】　渡邊　隆

【選任した代理人】

【識別番号】　100101465

【弁理士】

【氏名又は名称】　青山　正和

【選任した代理人】

【識別番号】　100094400

【弁理士】

【氏名又は名称】　鈴木　三義

【選任した代理人】

【識別番号】　100106493

【弁理士】

【氏名又は名称】　松冨　豊

【選任した代理人】

【識別番号】　100107836

【弁理士】

【氏名又は名称】　西　和哉

【選任した代理人】

【識別番号】　100108394

【弁理士】

【氏名又は名称】　今村　健一

【選任した代理人】

【識別番号】　100108453

【弁理士】

【氏名又は名称】　村山　靖彦

【選任した代理人】

【識別番号】　100100077

【弁理士】

【氏名又は名称】　大場　充

【手数料の表示】

【予納台帳番号】　008707

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704954

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化装置、復号化装置、方法及びその記録媒体

【特許請求の範囲】

【請求項１】　鍵暗号化部と、暗号化部とからなる暗号化装置において、

前記鍵暗号化部は、

共通鍵暗号方式を利用して暗号化に用いる共通鍵を取得または生成する共通鍵取得部と、

公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする共通鍵暗号化部と、

前記共通鍵より共通鍵改竄検出に利用する鍵情報を作成する第１共通鍵改竄検出情報作成部とからなり、

前記暗号化部は、

前記共通鍵を用いて平文を暗号化し暗号文とするデータ暗号化部と、

前記平文より第１データ改竄検出情報を作成する第１データ改竄検出情報作成部とからなる

ことを特徴とする暗号化装置。

【請求項２】　前記共通鍵暗号化部は、前記データ暗号化部により生成される暗号文を共有する利用者毎に、該利用者の公開鍵を用いて前記共通鍵を暗号化し暗号化共通鍵を生成する

ことを特徴とする請求項１記載の暗号化装置。

【請求項３】　前記暗号化装置は、鍵復号化部をさらに備え、

前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する共通鍵復号化部と、

前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第２共通鍵改竄検出情報作成部と、

前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第１改竄検証部とからなり、

前記鍵復号化部は、前記暗号化共通鍵を復号化し共通鍵を取得するとともに改竄検証し、

前記暗号化部は、前記共通鍵を用いて追加する平文をさらに暗号化する
ことを特徴とする請求項１または請求項２に記載の暗号化装置。

【請求項４】　請求項１に記載の暗号化装置によって暗号化された前記暗号化共通鍵と前記暗号文を復号化する、鍵復号化部と復号化部とからなる復号化装置において、

前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する共通鍵復号化部と、

前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第２共通鍵改竄検出情報作成部と、

前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第１改竄検証部とからなり、

前記復号化部は、共通鍵暗号方式を利用して前記暗号文を復号化するデータ復号化部と、

前記暗号文を復号化した平文より第２データ改竄検出情報を作成する第２データ改竄検出情報作成部と、

前記第１データ改竄検出情報と前記第２データ改竄検出情報を用いて改竄検証する第２改竄検証部とからなる
ことを特徴とする復号化装置。

【請求項５】　前記共通鍵復号化部は、暗号文を共有する利用者毎に対応する暗号化共通鍵のすべてを復号化し、

前記共通鍵改竄検出情報作成部は、復号化して得た共通鍵毎に前記共通鍵改竄検出情報を作成し、

前記第１改竄検証部は、前記鍵情報と前記共通鍵改竄検出情報から改竄検証を行なうとともに、利用者に対応する共通鍵を判定する
ことを特徴とする請求項４に記載の復号化装置。

【請求項６】　請求項１ないし請求項３のいずれかに記載の暗号化装置と、請求項４または請求項５に記載の復号化装置とから
構成される暗号化復号化装置。

【請求項７】　共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得また

は生成する手順と、

公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする手順と、

前記共通鍵より鍵情報を作成する手順と、

平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、

前記平文より第１データ改竄検出情報を作成する手順とを具備する

ことを特徴とする暗号化方法。

【請求項８】　公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する手順と、

前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、

前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、

前記暗号文を共通鍵暗号方式で復号化する手順と、

前記暗号文を復号化した平文より第２データ改竄検出情報を作成する手順と、

前記第１データ改竄検出情報と前記第２データ改竄検出情報とから改竄検証する手順とを具備する

ことを特徴とする復号化方法。

【請求項９】　共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得または生成する手順と、

公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする手順と、

前記共通鍵より鍵情報を作成する手順と、

平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、

前記平文より第１データ改竄検出情報を作成する手順とを

コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１０】　公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する手順と、

前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、

前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、

前記暗号文を共通鍵暗号方式で復号化する手順と、

前記暗号文を復号化した平文より第２データ改竄検出情報を作成する手順と、

前記第１データ改竄検出情報と前記第２データ改竄検出情報とから改竄検証する手順とを

コンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報の暗号化復号化を行なう暗号化装置、復号化装置、方法及びその記録媒体に関する。

【０００２】

【従来の技術】

一般に情報の伝達に際し、この情報に秘匿性が要求される場合がある。そこでさまざまな暗号化方式が考案されている。ここで従来の暗号化・著名方式を用いた暗号化装置の１例の動作フローチャートを図１５に示す。この例の方式では、公開鍵暗号方式と共通鍵暗号方式を組み合わせ利用している。

まず、暗号化装置は、送信者による共通鍵の入力か、または暗号化装置側で乱数を発生させ共通鍵を生成し共通鍵を取得する（ステップＳ１５１）。

次に、公開鍵暗号方式を利用し受信者の公開鍵を用いて共通鍵を暗号化し暗号化共通鍵とする（ステップＳ１５２）。

次に共通鍵暗号化方式を利用し、平文を共通鍵を用いて暗号化し暗号文を生成する（ステップＳ１５３）。

さらにハッシュ関数を用いて平文を圧縮することでメッセージダイジェストであるＭＤを作成する（ステップＳ１５４）。

そして、このＭＤを送信者の秘密鍵で暗号化することで電子署名を付加する（ステップＳ１５５）。

送信者は、以上で生成した暗号化共通鍵と暗号文と署名をネットワーク等を介して受信者に送信する。

【０００３】

図１６に、上記暗号化・署名方式に対応する復号化方式を用いた復号化装置の動作フローチャートを示す。

復号化装置は、暗号化共通鍵と暗号文と署名を受信すると、まず受信者の秘密鍵を利用して暗号化共通鍵を復号化し共通鍵を得る（ステップＳ１６１）。

そしてこの共通鍵を用いて暗号文を復号化し平文を得る（ステップＳ１６２）。

次に復号化して得た平文をハッシュ関数で圧縮しメッセージダイジェストＭＤ’を生成する（ステップＳ１６３）。

さらに受信したメッセージダイジェストＭＤの電子署名を送信者の公開鍵で復号化しＭＤを得る（ステップＳ１６４）。

次に、このＭＤと先のＭＤ’を比較し、元の平文が改竄されていないかの検証を行なっている。この方式の場合、著名検証により平文への著名者を本人確認できる利点がある。

【０００４】

次に、特開平８－１５６９６４に開示されている暗号化方式では、平文であるデータパーツが複数からなる情報を上記方式で暗号化している。図１７にｎ個のデータパーツ（平文）からなる情報と、この情報から生成される暗号化情報の構成を示している。この場合の暗号化情報は、各データパーツに対応する暗号化共通鍵とデータパーツの暗号文とデータパーツの署名を含んでいる。一例として６９バイトのデータパーツに対して付加される署名のサイズは、２３２９バイトである。署名のサイズには下限がありデータパーツのサイズが小さくても署名はあるサイズ以上の大きさをもつ。例えば、６９バイトのデータパーツ１００個から構成される情報に対し、改竄防止のために署名を付加すると、２３２９ｘ１００＝２３２９００バイトの情報が付加されることになる。

【０００５】

次に、特開平９－７１３８８に開示されている暗号化方式では、複数のデータパーツからなる情報に対して、各データパーツのメッセージダイジェストをまとめて署名し暗号化している。図１８にｎ個のデータパーツ（平文）からなる情報

と、この情報から生成される暗号化情報の構成を示している。

【０００６】

【発明が解決しようとする課題】

複数のデータパーツからなる情報を暗号化する場合、例えば特開平８－１５６９６４に開示されている方式では、データのオーバーヘッドが大きくなり、暗号化情報の伝送により多くの時間がかかることや、記憶装置等の資源を多く必要とする等の問題がある。また、特開平９－７１３８８に開示されている方式では、各データパーツのメッセージダイジェストをまとめて署名しているので、すべての平文がそろわないと署名の確認ができず、一部のデータパーツの参照のみ許可されているユーザがいる場合、データパーツの改竄を検証することができない点や、各データパーツを同時に変更できない等の問題がある。

【０００７】

本発明は、上記の点に鑑みてなされたもので、複数のデータパーツ（平文）を含む情報を暗号化した暗号化情報のオーバーヘッドをより少なくでき、また複数のユーザで利用可能であるとともに、各データパーツの改竄検証と同時変更も可能な暗号化装置、復号化装置、方法及びその記録媒体を提供するものである。

【０００８】

【課題を解決するための手段】

本発明の暗号化装置は、鍵暗号化部と、暗号化部とからなる暗号化装置において、前記鍵暗号化部は、共通鍵暗号方式を利用して暗号化に用いる共通鍵を取得または生成する共通鍵取得部と、公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする共通鍵暗号化部と、前記共通鍵より共通鍵改竄検出に利用する鍵情報を作成する第１共通鍵改竄検出情報作成部とからなり、前記暗号化部は、前記共通鍵を用いて平文を暗号化し暗号文とするデータ暗号化部と、前記平文より第１データ改竄検出情報を作成する第１データ改竄検出情報作成部とからなることを特徴とする。

【０００９】

前記共通鍵暗号化部は、前記データ暗号化部により生成される暗号文を共有する利用者毎に、該利用者の公開鍵を用いて前記共通鍵を暗号化し暗号化共通鍵を

生成することを特徴とする。

【００１０】

前記暗号化装置は、鍵復号化部をさらに備え、前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する共通鍵復号化部と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第２共通鍵改竄検出情報作成部と、前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第１改竄検証部とからなり、前記鍵復号化部は、前記暗号化共通鍵を復号化し共通鍵を取得するとともに改竄検証し、前記暗号化部は、前記共通鍵を用いて追加する平文をさらに暗号化することを特徴とする。

【００１１】

本発明の復号化装置は、請求項１に記載の暗号化装置によって暗号化された前記暗号化共通鍵と前記暗号文を復号化する、鍵復号化部と復号化部とからなる復号化装置において、前記鍵復号化部は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する共通鍵復号化部と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する第２共通鍵改竄検出情報作成部と、前記鍵情報と前記共通鍵改竄検出情報を用いて改竄検証する第１改竄検証部とからなり、前記復号化部は、共通鍵暗号方式を利用して前記暗号文を復号化するデータ復号化部と、前記暗号文を復号化した平文より第２データ改竄検出情報を作成する第２データ改竄検出情報作成部と、前記第１データ改竄検出情報と前記第２データ改竄検出情報を用いて改竄検証する第２改竄検証部とからなることを特徴とする。

【００１２】

前記共通鍵復号化部は、暗号文を共有する利用者毎に対応する暗号化共通鍵のすべてを復号化し、前記共通鍵改竄検出情報作成部は、復号化して得た共通鍵毎に前記共通鍵改竄検出情報を作成し、前記第１改竄検証部は、前記鍵情報と前記共通鍵改竄検出情報から改竄検証を行なうとともに、利用者に対応する共通鍵を判定することを特徴とする。

【００１３】

請求項６に記載の発明は、請求項１ないし請求項３のいずれかに記載の暗号化装置と、請求項４または請求項５に記載の復号化装置とから構成される暗号化復

号化装置である。

【００１４】

本発明の暗号化方法は、共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得または生成する手順と、公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする手順と、前記共通鍵より鍵情報を作成する手順と、平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、前記平文より第１データ改竄検出情報を作成する手順とを具備することを特徴とする。

【００１５】

本発明の復号化方法は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する手順と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、 前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、前記暗号文を共通鍵暗号方式で復号化する手順と、前記暗号文を復号化した平文より第２データ改竄検出情報を作成する手順と、前記第１データ改竄検出情報と前記第２データ改竄検出情報とから改竄検証する手順とを具備することを特徴とする。

【００１６】

請求項８に記載の発明は、共通鍵暗号方式を利用し、暗号化に用いる共通鍵を取得または生成する手順と、公開鍵暗号方式を利用して前記共通鍵を暗号化し暗号化共通鍵とする手順と、前記共通鍵より鍵情報を作成する手順と、平文を共通鍵暗号方式を利用して暗号化し暗号文とする手順と、前記平文より第１データ改竄検出情報を作成する手順とをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体からなる。

【００１７】

請求項９に記載の発明は、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する手順と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する手順と、前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する手順と、前記暗号文を共通鍵暗号方式で復号化する手順と、前記暗号文を復号化した平文より第２データ改竄検出情報を作成する手順と、前記第１データ改竄検出情報と前記第２データ改竄検出情報とから改竄検証する手順とをコンピュータに実

行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体からなる。

【００１８】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して説明する。

図１は、本発明の一実施形態である暗号化装置、復号化装置の構成を示すブロック図である。なお、本実施の形態では、暗号化装置と復号化装置とが一体となった暗号化復号化装置として説明する。

【００１９】

本実施形態の暗号化復号化装置１０は、鍵暗号化部１１と、鍵復号化部１２と、暗号化部１３と、復号化部１４とを備える。鍵暗号化部１１は、共通鍵取得部１５と共通鍵暗号化部１６と第１共通鍵改竄検出情報作成部としての共通鍵改竄検出情報作成部１７からなる。鍵復号化部１２は、共通鍵復号化部１８と第２共通鍵改竄検出情報作成部としての共通鍵改竄情報作成部１９と第１改竄検証部としての改竄検証部２０からなる。暗号化部１３は、データ暗号化部２１と第１データ改竄検出情報作成部としてのデータ改竄検出情報作成部２２からなる。復号化部１４は、データ復号化部２３と第２データ改竄検出情報作成部としてのデータ改竄検出情報作成部２４と第２改竄検証部としての改竄検証部２５からなる。

【００２０】

共通鍵取得部１５は、暗号化に使用する共通鍵を取得または生成する。共通鍵の生成には、一例として乱数生成装置等を利用し生成させる。共通鍵暗号化部１６は、ＲＳＡ方式や楕円暗号方式等の公開鍵暗号方式を利用して共通鍵を暗号化する。暗号化に使用する公開鍵は、情報を共有するメンバーの公開鍵を使用する。例えば共有メンバーが３人の場合、３人が所持する公開鍵を用いて共通鍵を暗号化し、３つの暗号化共通鍵を作成する。共通鍵改竄検出情報作成部１７は、共通鍵の正当性（①改竄されていない、②正当なユーザによって作成されている等）を検証するために利用する鍵情報を作成する。一例として、共通鍵をＭＤ５、ＳＨＡ－１等のハッシュ関数で圧縮して共通鍵のメッセージダイジェストＭＤを作成し、このＭＤに共通鍵作成者の秘密鍵を用いて署名を行なったものを鍵情報

として利用できる。署名の作成・検証には、公開鍵暗号方式の他、ＤＳＡ等のデジタル署名方式等を利用してよい。

【００２１】

共通鍵復号化部１８は、共通鍵暗号化部１６により暗号化された暗号化共通鍵を公開鍵暗号方式を用いて復号化する。復号化に用いる秘密鍵は、復号化を行なうユーザの秘密鍵を用いる。共通鍵改竄検出情報作成部１９は、共通鍵の正当性確認を行なうために利用する共通鍵改竄検出情報を作成する。例えば、共通鍵復号化部１８で復号化された共通鍵をハッシュ関数で圧縮したメッセージダイジェストＭＤ’を作成する。改竄検証部２０は、鍵情報（一例としてＭＤ）と共通鍵改竄検出情報作成部１９で作成した共通鍵改竄検出情報（一例としてＭＤ’）を比較検証することにより、共通鍵の正当性を確認する。共通鍵の正当性を確認するにあたり、共通鍵作成者自身の正当性確認も必要となるが、別途定められるものである。

【００２２】

データ暗号化部２１は、データパーツ（平文）を共通鍵暗号方式を利用して暗号化し、暗号文を生成する。暗号化に使用する共通鍵は、初めて暗号化する場合には共通鍵取得部１５で取得または生成された共通鍵を用い、既存の暗号化情報を利用する場合には、共通鍵復号化部１８により復号化された共通鍵を用いる。データ改竄検出情報作成部２２は、データパーツが改竄されていないか検証するための第１データ改竄検出情報を作成する。例えば、ハッシュ関数を用いてデータパーツを圧縮したメッセージダイジェストや、データパーツから抽出した部分情報、ＩＤ番号等などを第１データ改竄検出情報として利用できる。

【００２３】

データ復号化部２３は、共通鍵暗号方式を用いて暗号文を復号化する。復号化に用いる共通鍵は、共通鍵復号化部１８により復号化された共通鍵を用いる。データ改竄検出情報作成部２４は、第１データ改竄検出情報に対応しデータパーツが改竄されていないか検証するための第２データ改竄検出情報を作成する。例えば、データ復号化部２３で復号化された元のデータパーツをハッシュ関数を用いて圧縮して作成したメッセージダイジェストや、データパーツから抽出した部分

情報、ＩＤ番号等などを第２データ改竄検出情報として利用できる。改竄検証部２５は、第１データ改竄検出情報と第２データ改竄検出情報を比較検証することにより、復号化した元のデータパーツの正当性を確認する。

【００２４】

なお、共通鍵暗号化部１６とデータ暗号化部２１を、同一の装置、手段で実現してもよい。また、共通鍵復号化部１８とデータ復号化部２３を、同一の装置、手段で実現してもよい。また、共通鍵改竄検出情報作成部１７と１９、または、データ改竄検出情報作成部２２と２４を、同一の装置、手段で実現してもよい。同様に、共通鍵改竄検出情報作成部１７と１９及びデータ改竄検出情報作成部２２と２４のすべてを、同一の装置、手段で実現してもよい。また、改竄検証部２０と改竄検証部２５を、同一の装置、手段で実現してもよい。また、本実施の形態の暗号化復号化装置を、単一の装置としてではなく、各部が独立した装置、手段として実現し利用してもよい。なお、請求項１および請求項２に記載の暗号化装置は、鍵暗号化部１１と暗号化部１３とから構成できる。また、請求項３に記載の暗号化装置は、鍵暗号化部１１と暗号化部１３と鍵復号化部１２とから構成できる。請求項４および請求項５に記載の復号化装置は、鍵復号化部１２と復号化部１４とから構成できる。

【００２５】

図２に、本実施形態の暗号化復号化装置１０の一利用形態を示す。

本利用形態では、ネットワークに接続可能なサーバや他端末装置等からなる情報保管装置３０と、暗号化復号化装置１０を備える端末装置３１とがネットワークを介して接続されている。情報保管装置３０は、ハードディスク、光磁気ディスク等の不揮発性の記録装置を備え、暗号化情報として、暗号文、データ改竄検出情報、暗号化共通鍵、鍵情報および関連情報を保存可能とする。また、端末装置３１には、周辺機器として入力装置、表示装置等（いずれも図示せず）が接続されるものとする。ここで、入力装置とはキーボード、マウス等の入力デバイスのことをいう。表示装置とはＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）や液晶表示装置等のことをいう。なお、暗号化情報をローカルな端末装置３１に保管し、スタンドアローンで利用してもよい。

【００２６】

次に、このように構成された利用形態における本実施形態の暗号化復号化装置１０の動作について説明する。

まず、最初のデータパーツを暗号化する際の暗号化復号化装置１０の動作を図３に示す動作フローチャートを参照して説明する。なお、下記の説明における動作手順は、本実施形態の動作の一例であり、その処理の順序は固定されるものではなく他の順序で実施されてもよい。

【００２７】

始めに、共通鍵取得部１５が、暗号化復号化装置１０の外部からの入力により共通鍵を取得するかまたは共通鍵の生成を行なう（ステップＳ３０１）。

【００２８】

それから共通鍵暗号化部１６は、ネットワークを介して予め取得している利用者の公開鍵を利用して共通鍵を暗号化した暗号化共通鍵を生成する（ステップＳ３０２）。

【００２９】

さらに、共通鍵改竄検出情報作成部１７は、共通鍵作成者の秘密鍵等の共通鍵作成者に関する情報を共通鍵改竄検出情報としての鍵情報として作成する（ステップＳ３０３）。

【００３０】

データ暗号化部２１はデータパーツ１（平文）を暗号化し暗号文１を生成する（ステップＳ３０４）。

【００３１】

さらに、データ改竄検出情報作成部２２は、データパーツ１からデータパーツ１に関する情報であるデータ改竄検出情報１を作成する（ステップＳ３０５）。

なお、データパーツがｎ個からなる場合、ステップＳ３０４からステップＳ３０５の処理をｎ回繰り返す。

【００３２】

そして暗号文１、２、…、ｎ、データ改竄検出情報１、２、…、ｎ、鍵情報、暗号化共通鍵の組を暗号化情報として情報保管装置３０へ送信する（ステップＳ

３０６）。

【００３３】

なお、上記説明は利用者が１人で、使用する暗号化共通鍵が１種類の場合である。暗号化情報を共有する利用者が複数（例えばｍ人）である場合は、ステップＳ３０２で、各利用者毎の公開鍵を用いてｍ種の暗号化共通鍵を生成させる。すなわち、利用者毎に対応する暗号化共通鍵が生成されることになる。

図４に、暗号化前の情報の構成と、暗号化された暗号化情報の構成を示す。ここでは、暗号化前のデータパーツ１、２、…、ｎから、暗号化情報として、暗号文１、２、…、ｎとデータ改竄検出情報１、２、…、ｎと暗号化共通鍵１、２、…、ｍと鍵情報が作成されることを示している。

【００３４】

次に、複数（ｎ個）のデータパーツの暗号文を含む暗号化情報を復号化する際の暗号化復号化装置１０の動作を図５の動作フローチャートを参照して説明する。

なおこの処理は、暗号化共通鍵を作成する際に用いた公開鍵と対をなす秘密鍵を所有する者が行なえるものである。

【００３５】

まず、暗号化復号化装置１０は情報保管装置３０に記憶されている暗号化情報を取得する（ステップＳ５０１）。なお、暗号化情報に含まれる暗号化共通鍵は、ユーザ名やユーザＩＤ等により対応づけられ、利用者に対応した暗号化共通鍵が情報保管装置３０から暗号化復号化装置１０に送られるものとする。

【００３６】

そして共通鍵復号化部１８は、利用者の秘密鍵を用いて暗号化共通鍵を復号化し共通鍵を得る（ステップＳ５０２）。ここで利用者の秘密鍵は、予め入力されているものとする。

【００３７】

次に、共通鍵改竄検出情報作成部１９は、ステップＳ５０２で得た共通鍵から共通鍵改竄検出情報を作成する（ステップＳ５０３）。

【００３８】

そして改竄検証部２０は、取得した鍵情報と共通鍵改竄検出情報を比較検証し鍵作成者の正当性を検証する（ステップＳ５０４）。この場合、２つの情報が一致することで鍵作成者の正当性を判断できる。

【００３９】

ステップＳ５０４で、鍵作成者が正当であると判断された場合、ｎ個の暗号文とｎ個のデータ改竄検出情報の組を順に以下の処理を行なう。

まず、データ復号化部２３は暗号文を共通鍵を用いて復号化する（ステップＳ５０５）。

【００４０】

そして、データ改竄検出情報作成部２４は、復号化したデータパーツを用いてデータ改竄検出情報を作成する（ステップＳ５０６）。なお、ここで作成したデータ改竄検出情報を第１データ改竄検出情報と呼び、暗号化情報として保持されているデータ改竄検出情報を第２データ改竄検出情報と呼ぶことにする。

【００４１】

次に改竄検証部２５は、作成された第１データ改竄検出情報と暗号化情報の一部である第２データ改竄検出情報を比較し改竄が行われていないか検証する（ステップＳ５０７）。２つの情報が一致することで改竄が行われていないことが検証される。

【００４２】

ステップＳ５０７で、改竄がないと判断されれば復号化したデータパーツ（平文）を出力する（ステップＳ５０８）。

【００４３】

なお、以上の説明では、ユーザ名やユーザＩＤ等と暗号化共通鍵を対応づけることで、鍵復号化部１２が利用者に対応する暗号化共通鍵のみを用いるようにしている。複数の暗号化共通鍵がある（すなわち、暗号化情報を共有する利用者が複数存在する）場合、利用者に対応する暗号化共通鍵を得るその他の方法として、上記ステップＳ５０２～Ｓ５０４を以下のようにする。まず、ステップＳ５０２においてすべての暗号化共通鍵を復号化する。ステップＳ５０２で複数の暗号化共通鍵を復号化した場合、正式でないものも含めて複数の共通鍵が生成される

。ステップＳ５０３では、ステップＳ５０２で生成されたすべての共通鍵に対し共通鍵改竄検出情報を作成する。次に、ステップＳ５０４で、各共通鍵改竄検出情報と鍵情報とを比較検証する。すべての組み合わせが異なるとき改竄が行われていることがわかり、一致するものがあれば対応する共通鍵が正式の共通鍵であることがわかる。

【００４４】

次に、上述した、データパーツ１、２、…、ｎから暗号化情報を作成し情報保管装置３０に転送した段階から、ここではさらに上記の暗号化情報に情報を追加する際の暗号化復号化装置１０の動作を図６に示す動作フローチャートを参照して説明する。

【００４５】

先ず、暗号化情報が保管されている情報保管装置３０から暗号化共通鍵と鍵情報を取得する（ステップＳ６０１）。なお、暗号化情報に含まれる暗号化共通鍵は、ユーザ名やユーザＩＤ等により対応づけられ、利用者に対応した暗号化共通鍵が情報保管装置３０から暗号化復号化装置１０に送られるものとする。

【００４６】

そして、共通鍵復号化部１８は、利用者の秘密鍵を用いて利用者に対応する暗号化共通鍵を復号化する（ステップＳ６０２）。ここで利用者の秘密鍵は、予め入力されているものとする。

【００４７】

次に、共通鍵改竄検出情報作成部１９は、ステップＳ６０２で得た共通鍵から共通鍵改竄検出情報を作成する（ステップＳ６０３）。

【００４８】

改竄検証部２０は、先の鍵情報と共通鍵改竄検出情報が一致するか比較検証し、鍵作成者の正当性を検証する（ステップＳ６０４）。この場合、２つの情報が一致することで鍵作成者の正当性を判断できる。

【００４９】

ステップＳ６０４で、鍵作成者が正当であると判断された場合、データ暗号化部２１は追加するデータパーツｎ＋１を暗号化し暗号文ｎ＋１を生成する（ステ

ップＳ６０５）。

【００５０】

さらにデータ改竄検出情報作成部２２はデータパーツｎ＋１から改竄検出情報ｎ＋１を作成する（ステップＳ６０６）。

なお、追加するデータパーツがＬ個からなる場合、ステップＳ６０５からステップＳ６０６の処理をＬ回繰り返す。

【００５１】

そして暗号文ｎ＋１、ｎ＋２、…、ｎ＋Ｌと改竄検出情報ｎ＋１、ｎ＋２、…、ｎ＋Ｌを情報保管装置３０に転送し暗号化情報として追加保管する（ステップＳ６０７）。

【００５２】

なお、以上の説明では、ユーザ名やユーザＩＤ等と暗号化共通鍵を対応づけることで、鍵復号化部１２が利用者に対応する暗号化共通鍵のみを用いるようにしている。複数の暗号化共通鍵がある（すなわち、暗号化情報を共有する利用者が複数存在する）場合、利用者に対応する暗号化共通鍵を得るその他の方法として、上記ステップＳ６０２～Ｓ６０４を以下のようにする。まず、ステップＳ６０２においてすべての暗号化共通鍵を復号化する。ステップＳ６０２で複数の暗号化共通鍵を復号化した場合、正式でないものも含めて複数の共通鍵が生成される。ステップＳ６０３では、ステップＳ６０２で生成されたすべての共通鍵に対し共通鍵改竄検出情報を作成する。次に、ステップＳ６０４で、各共通鍵改竄検出情報と鍵情報とを比較検証する。すべての組み合わせが異なるとき改竄が行われていることがわかり、一致するものがあれば対応する共通鍵が正式の共通鍵であることがわかる。

図７に、暗号化情報の追加前の構成と、追加後の構成を示す。ここでは、暗号化情報として、暗号文ｎ＋１、ｎ＋２、…、ｎ＋Ｌとデータ改竄検出情報ｎ＋１、ｎ＋２、…、ｎ＋Ｌがもとの暗号化情報に追加されていることを示している。

【００５３】

次に、情報保管装置３０に記憶されている暗号化情報を共有しているチームに、共有メンバーを追加する際の暗号化復号化装置１０の動作を図８に示す動作フ

ローチャートを参照して説明する。ここでは、共有メンバーＡ、Ｂが所属しているチームに、共有メンバーＢが、新しい共有メンバーとして共有メンバーＣを追加する場合を説明する。

【００５４】

まず、共有メンバーＢの操作により、暗号化復号化装置１０は情報保管装置３０にアクセスし、鍵情報と共有メンバーＢに対応する暗号化共通鍵Ｂを取得する（ステップＳ８０１）。

【００５５】

共通鍵復号化部１８は、受信者である共有メンバーＢの秘密鍵を用いて暗号化共通鍵Ｂを復号化し、共通鍵を得る（ステップＳ８０２）。

【００５６】

共通鍵改竄検出情報作成部１９は共通鍵から共通鍵改竄検出情報を作成する（ステップＳ８０３）。

【００５７】

そして改竄検証部２０は、取得した鍵情報と共通鍵改竄検出情報を比較検証し鍵作成者の正当性を確認する（ステップＳ８０４）。この場合、２つの情報が一致することで改竄が行われていないことが検証される。

【００５８】

ステップＳ８０４で、鍵作成者の正当性が確認されると、共通鍵暗号化部１６は共有メンバーとして追加する共有メンバーＣの公開鍵を用いて共通鍵を暗号化し、暗号化共通鍵Ｃを生成する（ステップＳ８０５）。

【００５９】

鍵暗号化部１２は生成された暗号化共通鍵Ｃを情報保管装置３０へ転送する（ステップＳ８０６）。

【００６０】

こうして、情報保管装置３０には３人の共有メンバーに対応する暗号化共通鍵Ａ、Ｂ、Ｃが保管されることになり、以後、追加された共有メンバーＣは、チームの暗号化情報に対する参照・変更等を行なえるようになる。

図９に、共有メンバーＣの追加前の暗号化情報の構成と、追加後の構成を示す

。ここでは、暗号化情報として、あらたな共有メンバーである共有メンバーＣ用の暗号化共通鍵Ｃがもとの暗号化情報に追加されていることを示している。

【００６１】

次に、共有メンバーを削除する際の暗号化復号化装置１０の動作を図１０に示す動作フローチャートを参照して説明する。ここでは、共有メンバーＡ、Ｂ、Ｃが所属しているチームにおいて、共有メンバーＢが共有メンバーＡを削除する場合を説明する。

【００６２】

暗号化復号化装置１０は、共有メンバーＢの入力操作による共有メンバーＡを削除するための削除命令を取得する（ステップＳ１０１）。

【００６３】

データ改竄検出情報作成部２２は、共有メンバーＡの削除命令に対応するデータ改竄検出情報を作成する（ステップＳ１０２）。

【００６４】

次に、暗号化復号化装置１０は、共有メンバーの削除命令と、削除命令を出した本人を識別する識別情報となるデータ改竄検出情報の組からなる削除情報を情報保管装置３０に転送する（ステップＳ１０３）。

【００６５】

なお、情報保管装置３０は、削除命令を出した本人を識別する機能をもち、削除命令に応じた暗号化共通鍵を削除できるものとする。また、ここで用いるデータ改竄検出情報として、共有メンバーＡの削除命令に対する共有メンバーＢの電子署名を用いてもよい。また、削除命令を出した本人を識別する識別情報としてＩＤ、パスワード等を用い情報保管装置３０が、情報保管装置３０に登録されている識別情報とを照合するようにしてもよい。

図１１に、共有メンバーＡの削除前の暗号化情報の構成と、削除後の構成を示す。ここでは、暗号化情報として、共有メンバーＡ用の暗号化共通鍵Ａがもとの暗号化情報から削除されていることを示している。

【００６６】

次に本実施形態の暗号化復号化装置１０の動作を具体例をあげて詳細に説明す

る。

まず第１の実施例として、ユーザＢが、チーム１０１（ユーザＡ、Ｂ、Ｃの３人が所属）で共有しているスケジュールの１９９８年の１０月１日の項目に用件「セミナー参加」と「１５：００」を加える際の処理を説明する。なお本実施例では、スケジュールに関する情報は暗号化情報と暗号化されていない情報を含み、外部の情報保管装置３０に保管されているものとする。また情報保管装置３０は、ユーザのアクセス権に応じて保管されている情報に対するアクセスを制限できるものとする。また、ユーザＢが使用する暗号化復号化装置１０は、ユーザＢによるデータの入力を受け付ける入力部（図示せず）と、情報を表示する表示部（図示せず）を備えているものとする。

【００６７】

まず、ユーザＢは暗号化復号化装置１０から情報保管装置３０にアクセスし、チーム１０１の１９９８年１０月のスケジュールにアクセスできるか確認する。

【００６８】

アクセス可能である場合、チーム１０１の１９９８年１０月のスケジュールにアクセスする。情報保管装置３０は、チーム１０１の１９９８年１０月のスケジュールを暗号化復号化装置１０に転送し、暗号化復号化装置１０はその表示部にスケジュールを表示する。なお、この段階ではスケジュールの情報はまだ暗号化されていないものとする。

【００６９】

ユーザＢは、暗号化復号化装置１０の入力部を用いて１９９８年の１０月１日の項目に「セミナー参加」と「１５：００～」を入力する。

【００７０】

次に、共通鍵暗号化部１６において共通鍵を生成する。本実施例ではこの共通鍵をｃＫｅｙ１と呼ぶことにする。

【００７１】

次に、共通鍵暗号化部１６で、ユーザＡ、ユーザＢ、ユーザＣの公開鍵を利用して、例えば公開鍵暗号方式であるＲＳＡ方式で暗号化する。こうして共通鍵暗号化部では、３人のユーザに対応して３つの暗号化共通鍵が生成される。本実施

例ではこれらの暗号化共通鍵をそれぞれ、ｅＫｅｙ１Ａ、ｅＫｅｙ１Ｂ、ｅＫｅｙ１Ｃと呼ぶことにする。

【００７２】

次に、共通鍵改竄検出情報作成部１７は、共通鍵のメッセージダイジェストであるＭＤを作成し、さらにこのＭＤにユーザＢの秘密鍵を利用して署名を行なう。この署名を行なったＭＤが鍵情報であるＳｉｇｎｅｄＫｅｙ１である。

【００７３】

データ暗号化部２１は、スケジュールのデータパーツである「セミナー参加」を共通鍵ｃＫｅｙ１で暗号化を行ない、暗号文ＣｒｙｐｔＤａｔａ１を生成する。

【００７４】

次に、データ改竄検出情報作成部２２は、一例としてハッシュ関数であるＭＤ５を利用して「セミナー参加」のメッセージダイジェストＭｅｓｓａｇｅＤ１を生成する。

【００７５】

「セミナー参加」に適用した手順をスケジュールのデータパーツである「１５：００～」に対して行ない、「１５：００～」の暗号文ＣｒｙｐｔＤａｔａ２とメッセージダイジェストＭｅｓｓａｇｅＤ２を得る。

【００７６】

そしてこれらの情報を暗号化復号化装置１０から情報保管装置３０に転送する。

なお、このときの情報保管装置３０に記憶される情報の構成を図１２に示す。上記処理で作成されたスケジュールを区別する情報、ユーザＩＤと暗号化共通鍵、鍵情報、暗号文とデータ改竄検出情報および関連情報が記憶される。

【００７７】

次に第２の実施例として、第１の実施例からさらに、第１の実施例で作成された暗号化情報にユーザＡが、チーム１０１（ユーザＡ、Ｂ、Ｃの３人が所属）で共有しているスケジュールの１９９８年の１０月２日の項目に用件「会議」と「１７：００～」を加える際の処理を説明する。

【００７８】

まず、ユーザＡは暗号化復号化装置１０から情報保管装置３０にアクセスし、チーム１０１の１９９８年１０月のスケジュールにアクセスできるか確認する。

【００７９】

アクセス可能である場合、チーム１０１の１９９８年１０月のスケジュールにアクセスする。情報保管装置３０は、暗号化共通鍵ｅＫｅｙ１Ａと鍵情報ＳｉｇｎｅｄＫｅｙ１を暗号化復号化装置１０に転送する。

【００８０】

ユーザＡは、暗号化復号化装置１０の入力部を用いて１９９８年の１０月２日の用件項目に「会議」と「１７：００～」を入力する。

【００８１】

次に、共通鍵復号化部１８は、ユーザＡの秘密鍵を用いて暗号化共通鍵ｅＫｅｙ１Ａを復号化し共通鍵ｃＫｅｙ１を生成する。

【００８２】

次に、共通鍵改竄検出情報作成部１９は、共通鍵ｃＫｅｙ１のメッセージダイジェストｋｅｙＤ１’を作成する。

【００８３】

次に、改竄検証部２０は、鍵情報のＳｉｇｎｅｄＫｅｙ１をユーザＢの公開鍵を利用して復号化し、暗号化前の共通鍵のメッセージダイジェストｋｅｙＤ１を得る。そして、ｋｅｙＤ１とｋｅｙＤ１’を比較する。ｋｅｙＤ１とｋｅｙＤ１’が等しければ、チーム１０１に所属するユーザＢによって作成された共通鍵を改竄されることなく取得できたことがわかる。こうして共通鍵の正当性が確認できる。ここで、ユーザＢが共通鍵を作成することが正当であるかどうか、すなわち、共通鍵作成者自身の正当性確認は、共通鍵作成者正当性確認用情報として取得する必要がある。この場合の共通鍵作成者正当性確認用情報の取得方法の一例としては、共通鍵作成者がユーザＢであることを暗号化復号化装置１０の表示部にダイアログボックスとして表示し、ユーザに確認してもらう方法をとってもよい。または、ネットワークを介して情報保管装置３０から関連情報として取得してもよい。

【００８４】

次に、データ暗号化部２１は、スケジュールのデータパーツである「会議」を共通鍵ｃＫｅｙ１で暗号化を行ない、暗号文ＣｒｙｐｔＤａｔａ３を生成する。

【００８５】

次に、データ改竄検出情報作成部２２は、一例としてハッシュ関数であるＭＤ５を利用して「会議」のメッセージダイジェストＭｅｓｓａｇｅＤ３を生成する。

【００８６】

「会議」に適用した手順をスケジュールのデータパーツである「１７：００～」に対して行ない、「１７：００～」の暗号文ＣｒｙｐｔＤａｔａ４とメッセージダイジェストＭｅｓｓａｇｅＤ４を得る。

【００８７】

そしてこれらの情報を暗号化復号化装置１０から情報保管装置３０に転送する。

なお、このときの情報保管装置３０に記憶される情報の構成を図１３に示す。上記処理で暗号文とデータ改竄検出情報が追加されているところを示している。

【００８８】

次に第３の実施例として、第１、第２の実施例で作成され情報保管装置３０に保管されているチーム１０１の１９９８年１０月のスケジュールをユーザＣが参照する場合の処理を説明する。

【００８９】

まず、ユーザＣは暗号化復号化装置１０から情報保管装置３０にアクセスし、チーム１０１の１９９８年１０月のスケジュールにアクセスできるか確認する。

【００９０】

アクセス可能である場合、チーム１０１の１９９８年１０月のスケジュールにアクセスする。情報保管装置３０は、チーム１０１の１９９８年１０月のスケジュールと暗号化共通鍵ｅＫｅｙ１Ｃと鍵情報ＳｉｇｎｅｄＫｅｙ１を暗号化復号化装置に転送する。

【００９１】

共通鍵復号化部１８は、ユーザＣの秘密鍵を用いて暗号化共通鍵ｅＫｅｙ１Ｃを復号化し共通鍵ｃＫｅｙ１を得る。

【００９２】

次に、共通鍵改竄検出情報作成部１９で、共通鍵ｃＫｅｙ１のメッセージダイジェストｃＫｅｙＤ’を作成する。

【００９３】

改竄検証部２０では、ＳｉｇｎｅｄＫｅｙ１をＢの公開鍵を用いて復号化し、暗号化前の共通鍵のメッセージダイジェストｃＫｅｙＤを得る。そして、このメッセージダイジェストｃＫｅｙＤと先のメッセージダイジェストｃＫｅｙＤ’を比較する。この２つのメッセージダイジェストが等しければチーム１０１に所属するユーザＢによって作成された共通鍵ｃＫｅｙ１を改竄されることなく取得できたことが検証できる。すなわち、取得した共通鍵の正当性を確認することができる。また、ここで共通鍵作成者自身の正当性確認を行なう必要があるが、第２の実施例で説明したとうりである。

【００９４】

次に、データ復号化部２３は、暗号文ＣｒｙｐｔＤａｔａ１を共通鍵復号化部１８より取得した共通鍵ｃＫｅｙ１を用いて復号化を行なう。ここで平文「セミナー参加」が得られる。

【００９５】

次に、データ改竄検出情報作成部２４で、ハッシュ関数の１つであるＭＤ５を用いて平文のメッセージダイジェストＭｅｓｓａｇｅＤ１’を生成する。

【００９６】

情報保管装置３０より転送されてきたメッセージダイジェストＭｅｓｓａｇｅＤ１とデータ改竄検出情報作成部２４で生成されたメッセージダイジェストＭｅｓｓａｇｅＤ１’を比較する。これら２つのメッセージダイジェストが等しければチーム１０１に所属する者によって作成されたデータパーツを改竄されることなく取得できたことがわかる。

【００９７】

同様の手順を繰り返すことで暗号文ＣｒｙｐｔＤａｔａ２…ＣｒｉｐｔＤａｔ

ａ４に対して行なうと、「１５：００～」、「会議」、「１７：００～」を得ることができる。復号化後のスケジュールの表示例を図１４に示す。図に示すようにユーザＢが入力したデータパーツ「セミナー参加」、「１５：００～」とユーザＡが入力したデータパーツ「会議」、「１７：００～」を同じチームに所属するユーザＣは見ることができる。

【００９８】

以上のように、１つのチームに所属する共有メンバーは、暗号化情報に対するデータパーツの追加や変更、他共有メンバーのデータパーツの参照等、自由に行なえるが、共有メンバー以外の者に対して秘匿性を保つことができる。

【００９９】

また一例として、ＭｅｓｓａｇｅＤ１、…、ＭｅｓｓａｇｅＤ４の各サイズを１６バイト、鍵情報のサイズを２３００バイト（下限がある）であるとすると、本実施例では

１６ｘ４＋２３００＝２３６４バイト

がオーバーヘッドとなる。

従来の方式で４つの暗号文のそれぞれに署名を付ける場合では

２３００ｘ４＝９２００バイト

のオーバーヘッドとなり、本発明の方式が従来方式より情報量を抑えることができている。

【０１００】

なお、本発明は、インターネットの他、ＬＡＮやダイアルアップによるネットワークを利用してもよい。

また、本発明の暗号化装置、復号化装置、及び方法を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより暗号化、復号化の処理を行ってもよい。

すなわち、暗号化プログラムを記録したコンピュータ読み取り可能な記録媒体において、暗号化プログラムは、共通鍵暗号方式を利用して暗号化に用いる共通鍵を取得または生成する機能と、公開鍵暗号方式を利用して前記共通鍵を暗号化

し暗号化共通鍵とする機能と、前記共通鍵より鍵情報を作成する機能と、平文を共通鍵暗号方式を利用して暗号化し暗号文とする機能と、前記平文より第１データ改竄検出情報を作成する機能をコンピュータに実現させる。

また、復号化プログラムを記録したコンピュータ読み取り可能な記録媒体において、復号化プログラムは、公開鍵暗号方式を利用して前記暗号化共通鍵を復号化する機能と、前記暗号化共通鍵を復号化した共通鍵より共通鍵改竄検出情報を作成する機能と、前記鍵情報と前記共通鍵改竄検出情報とから改竄検証する機能と、前記暗号文を共通鍵暗号方式で復号化する機能と、前記暗号文を復号化した平文より第２データ改竄検出情報を作成する機能と、前記第１データ改竄検出情報と前記第２データ改竄検出情報とから改竄検証する機能をコンピュータに実現させる。

【０１０１】

なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピーディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可般媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。

【０１０２】

以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【０１０３】

【発明の効果】

以上、詳細に説明したように、本発明によれば平文毎に改竄検出情報を作成することはせず、各平文を暗号化する共通鍵に対して改竄検出情報となる鍵情報を作成し、改竄検出と共通鍵作成者の本人確認を可能としたので、情報を暗号化した暗号化情報のオーバーヘッドを減少させることができる。したがって、暗号化情報の転送時におけるネットワークにかかる負荷と暗号化情報を保管する際に要する記憶装置の容量を減少させることができる。また、各平文に第１データ改竄検出情報を付加したので、個々の平文毎に改竄検出が可能である。また、利用者毎に暗号化共通鍵を作成することで複数の利用者間で暗号化情報を共有できる。

【図面の簡単な説明】

【図１】　本発明の一実施形態である暗号化復号化装置の構成を示すブロック図である。

【図２】　本発明の一利用形態を示す図である。

【図３】　暗号化に係る動作を説明するフローチャートである。

【図４】　暗号化前の情報と暗号化情報の構成を示す図である。

【図５】　復号化に係る動作を説明するフローチャートである。

【図６】　暗号化情報に情報を追加する際の動作を説明するフローチャートである。

【図７】　暗号化情報に情報を追加する前後の暗号化情報の構成を示す図である。

【図８】　共有メンバーＢが、チームに共有メンバーＣを追加する際の動作を説明するフローチャートである。

【図９】　チームに共有メンバーＣを追加する前後の暗号化情報の構成を示す図である。

【図１０】　チームから共有メンバーを削除する際の動作を説明するフローチャートである。

【図１１】　チームから共有メンバーＡを削除する前後の暗号化情報の構成を示す図である。

【図１２】　第１の実施例における情報保管装置に記憶されている情報を示

す図である。

【図１３】　第２の実施例において情報を追加した際の情報保管装置に記憶されている情報を示す図である。

【図１４】　第３の実施例において復号化後のスケジュールの表示例を示す図である。

【図１５】　従来の暗号化・署名方式における暗号化の動作を説明するフローチャートである。

【図１６】　従来の暗号化・署名方式における復号化の動作を説明するフローチャートである。

【図１７】　特開平８－１５６９６４に開示されている暗号化方式による暗号化前の情報と暗号化情報の構成を示す図である。

【図１８】　特開平９－７１３８８に開示されている暗号化方式による暗号化前の情報と暗号化情報の構成を示す図である。

【符号の説明】

１０…暗号化復号化装置　　１１…鍵暗号化部

１２…鍵復号化部　　１３…暗号化部

１４…復号化部　　１５…共通鍵取得部

１６…共通鍵暗号化部　　１７…共通鍵改竄検出情報作成部

１８…共通鍵復号化部　　１９…共通鍵改竄検出情報作成部

２０…改竄検証部　　２１…データ暗号化部

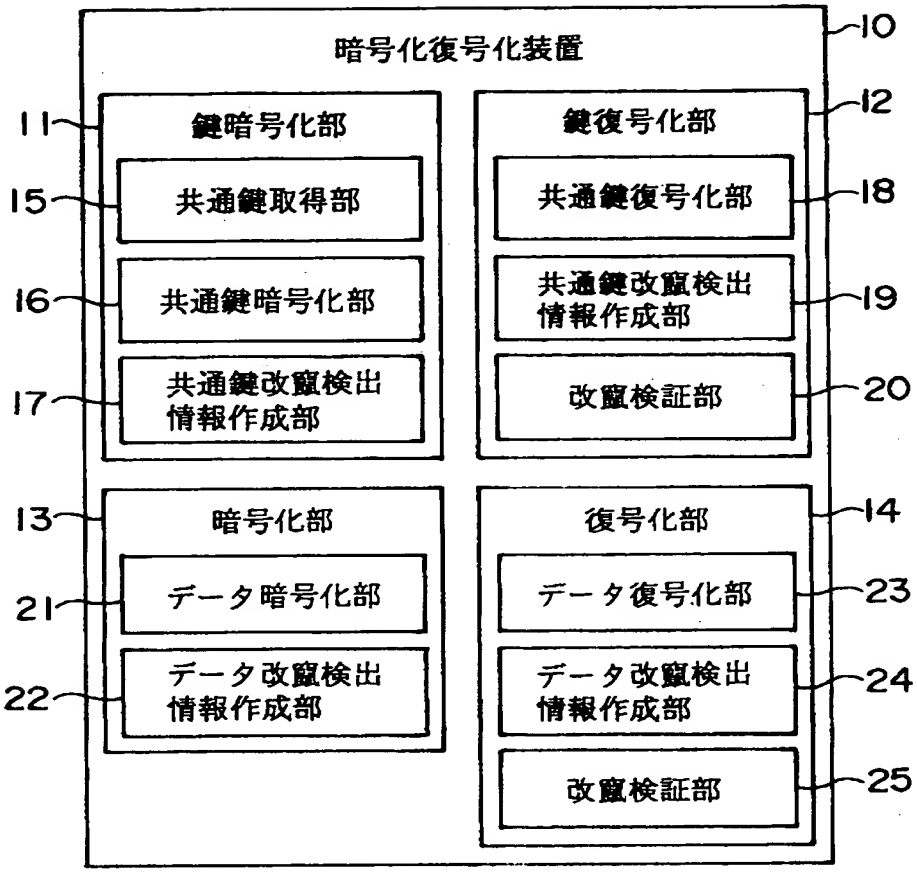
２２…データ改竄検出情報作成部　　２３…データ復号化部

２４…データ改竄検出情報作成部　　２５…改竄検証部

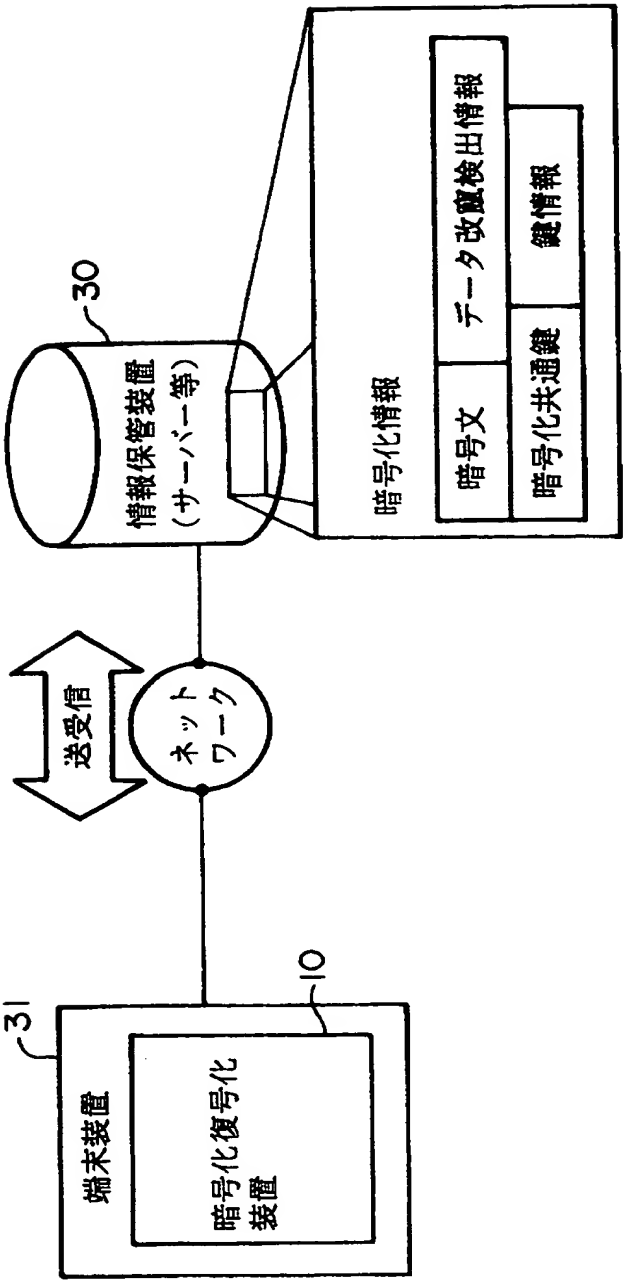
３０…情報保管装置　　３１…端末装置

【書類名】　　図面

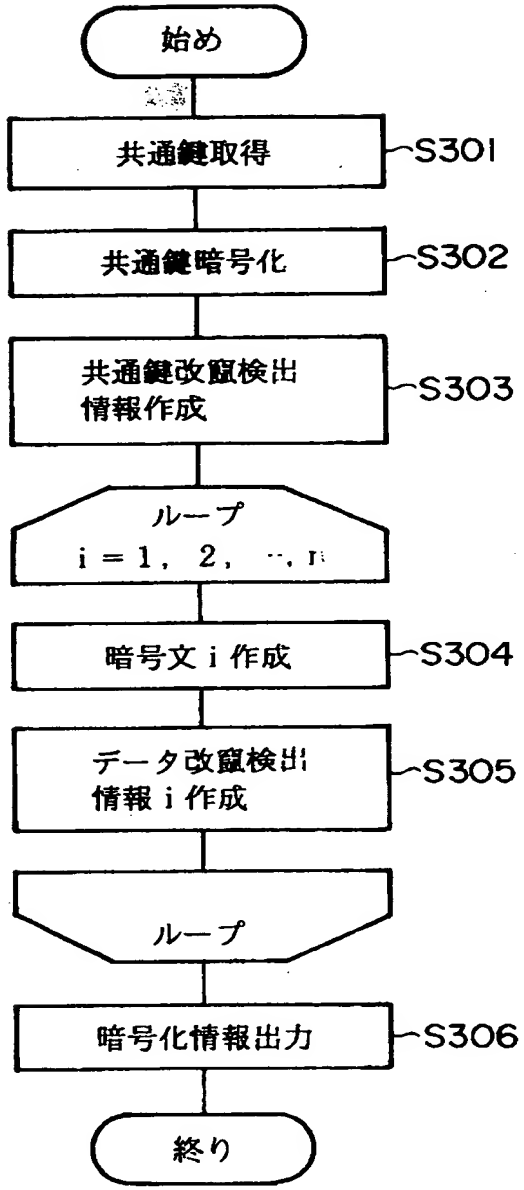
【図１】


暗号化復号化装置
10
鍵暗号化部
11
共通鍵取得部
15
共通鍵暗号化部
16
共通鍵改竄検出情報作成部
17
鍵復号化部
12
共通鍵復号化部
18
共通鍵改竄検出情報作成部
19
改竄検証部
20
暗号化部
13
データ暗号化部
21
データ改竄検出情報作成部
22
復号化部
14
データ復号化部
23
データ改竄検出情報作成部
24
改竄検証部
25

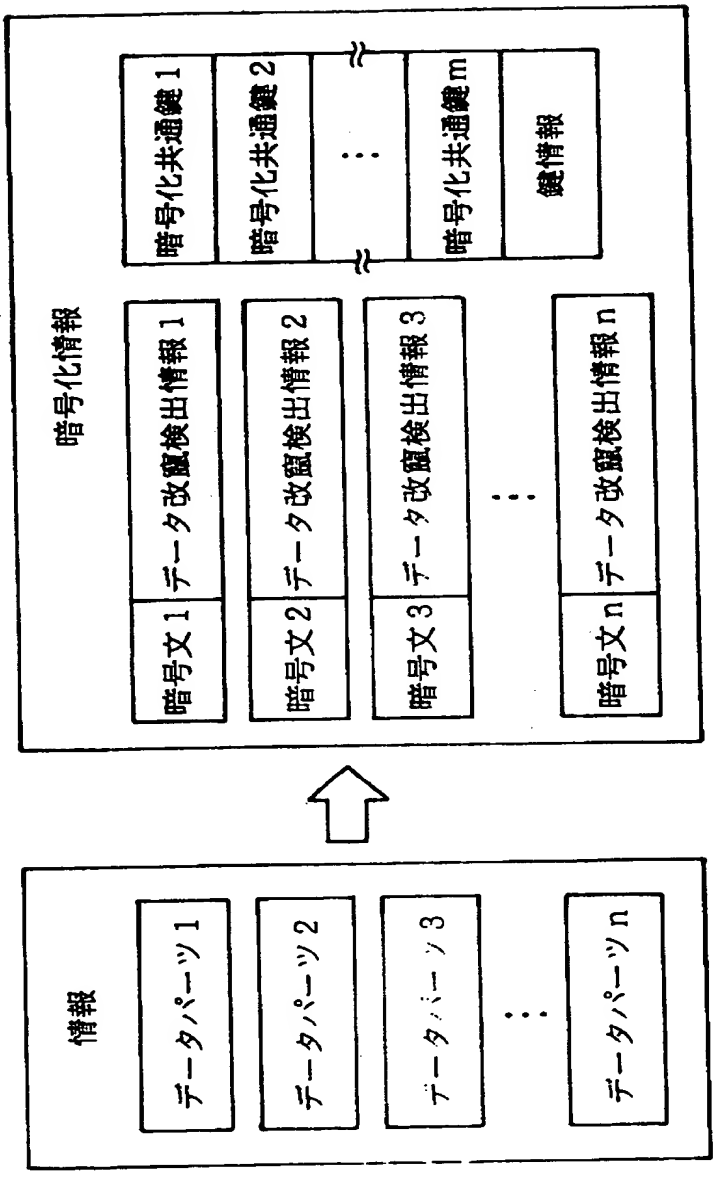
【図２】


30
情報保管装置
（サーバー等）
暗号化情報
暗号文
暗号化共通鍵
データ改竄検出情報
鍵情報
送受信
ネットワーク
31
端末装置
10
暗号化復号化
装置

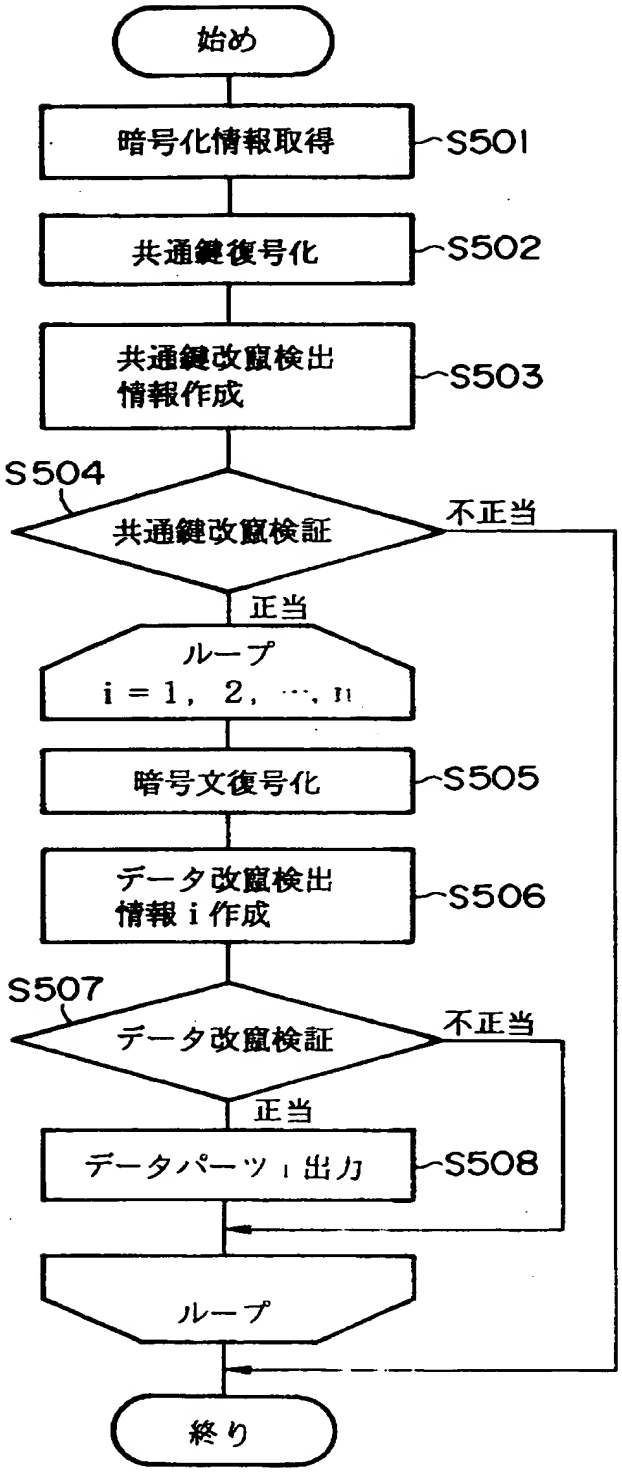
【図３】


始め
共通鍵取得
S301
共通鍵暗号化
S302
共通鍵改竄検出
情報作成
S303
ループ
i＝1，2，…，n
暗号文ｉ作成
S304
データ改竄検出
情報ｉ作成
S305
ループ
暗号化情報出力
S306
終り

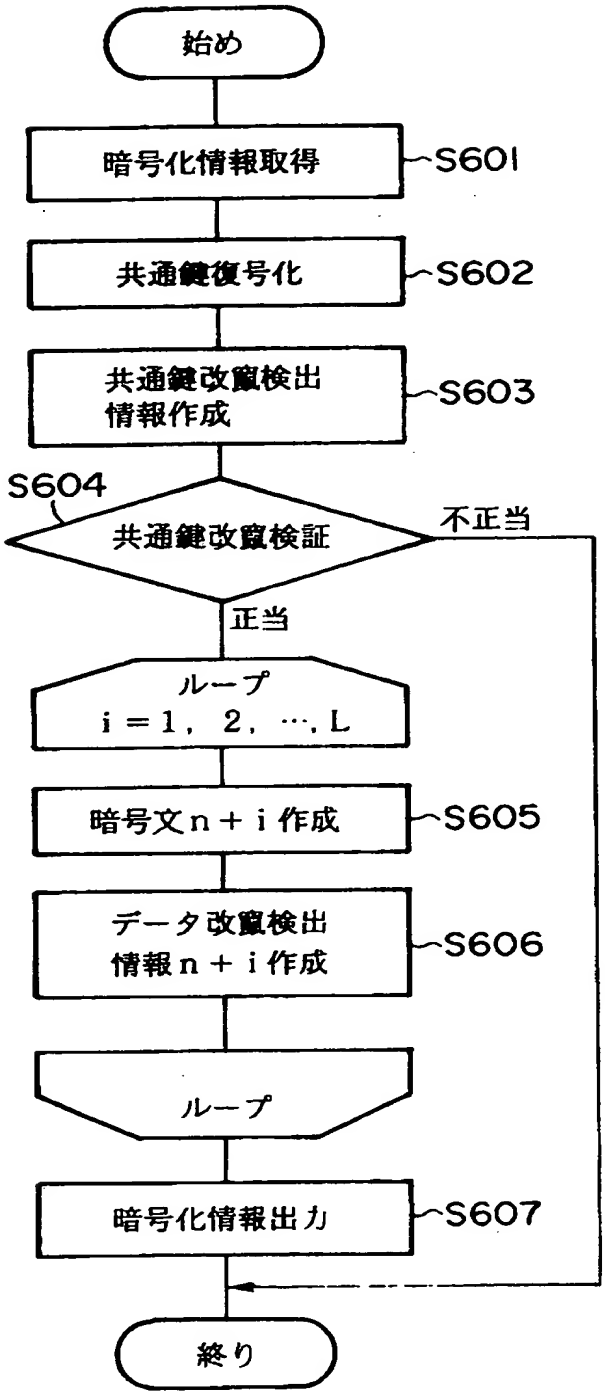
【図４】


暗号化情報
暗号化共通鍵１
暗号化共通鍵２
暗号化共通鍵ｍ
鍵情報
暗号文１
データ改竄検出情報１
暗号文２
データ改竄検出情報２
暗号文３
データ改竄検出情報３
暗号文ｎ
データ改竄検出情報ｎ
情報
データパーツ１
データパーツ２
データパーツ３
データパーツｎ

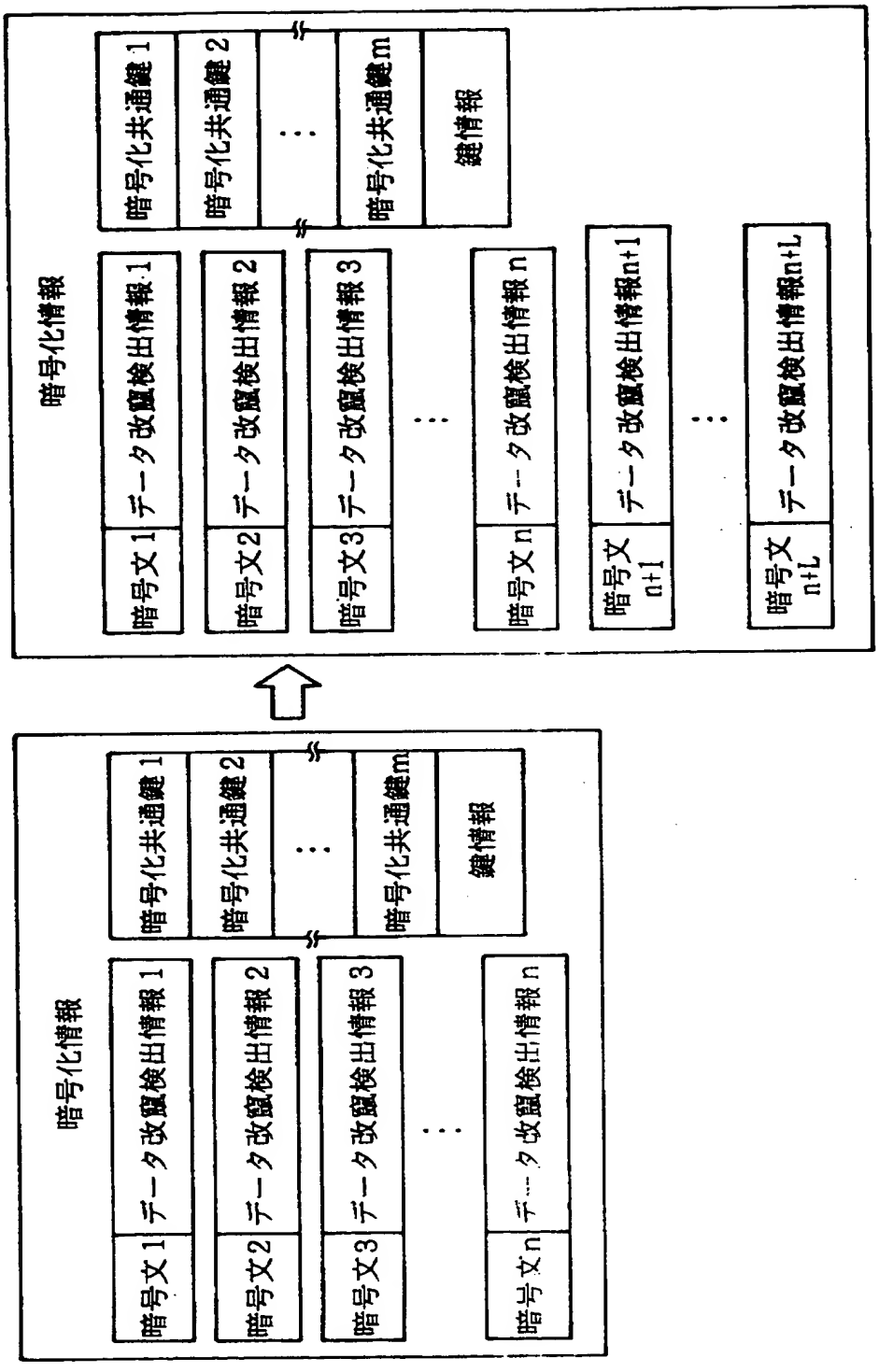
【図５】


始め
暗号化情報取得
S501
共通鍵復号化
S502
共通鍵改竄検出
情報作成
S503
S504
共通鍵改竄検証
不正当
正当
ループ
i＝1，2，…，n
暗号文復号化
S505
データ改竄検出
情報ｉ作成
S506
S507
データ改竄検証
不正当
正当
データパーツｉ出力
S508
ループ
終り

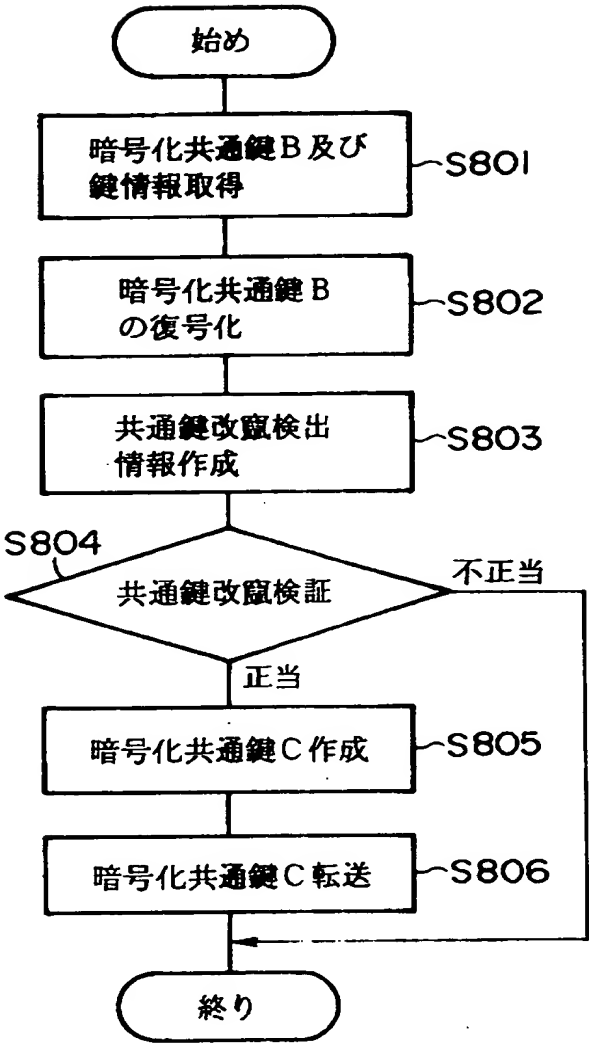
【図６】


始め
暗号化情報取得
S601
共通鍵復号化
S602
共通鍵改竄検出
情報作成
S603
S604
共通鍵改竄検証
不正当
正当
ループ
i＝1，2，…，L
暗号文n＋i作成
S605
データ改竄検出
情報n＋i作成
S606
ループ
暗号化情報出力
S607
終り

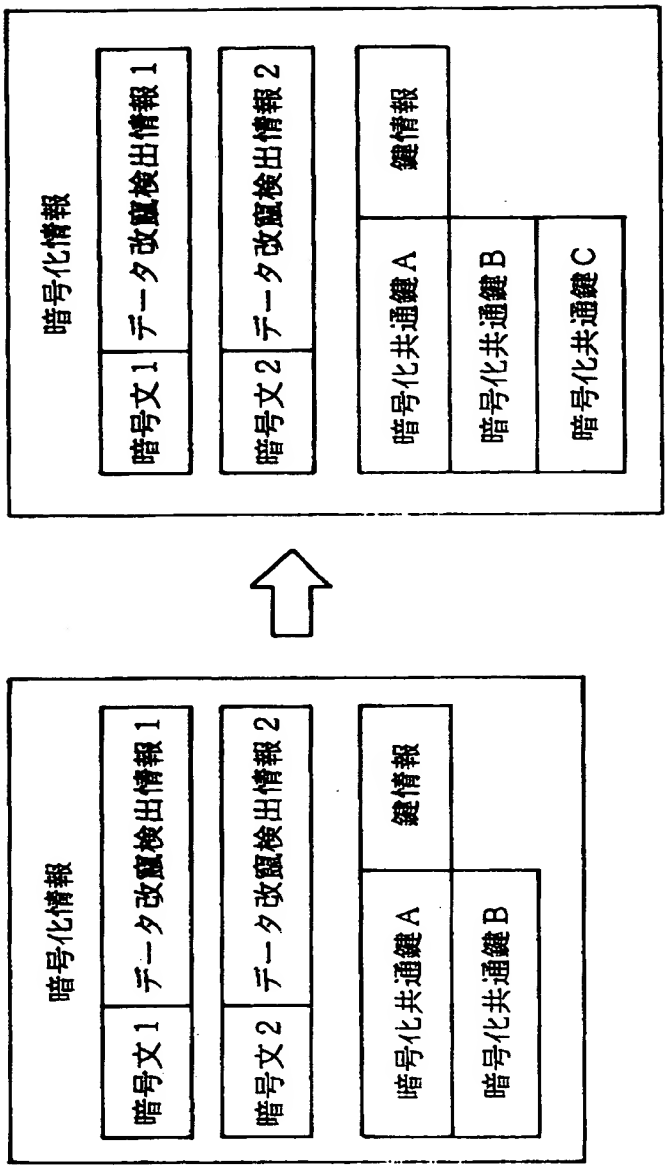
【図７】


暗号化情報
暗号文1
データ改竄検出情報1
暗号文2
データ改竄検出情報2
暗号文3
データ改竄検出情報3
暗号文n
データ改竄検出情報n
暗号化共通鍵1
暗号化共通鍵2
暗号化共通鍵m
鍵情報
暗号化情報
暗号文1
データ改竄検出情報1
暗号文2
データ改竄検出情報2
暗号文3
データ改竄検出情報3
暗号文n
データ改竄検出情報n
暗号文 n+1
データ改竄検出情報n+1
暗号文 n+L
データ改竄検出情報n+L
暗号化共通鍵1
暗号化共通鍵2
暗号化共通鍵m
鍵情報

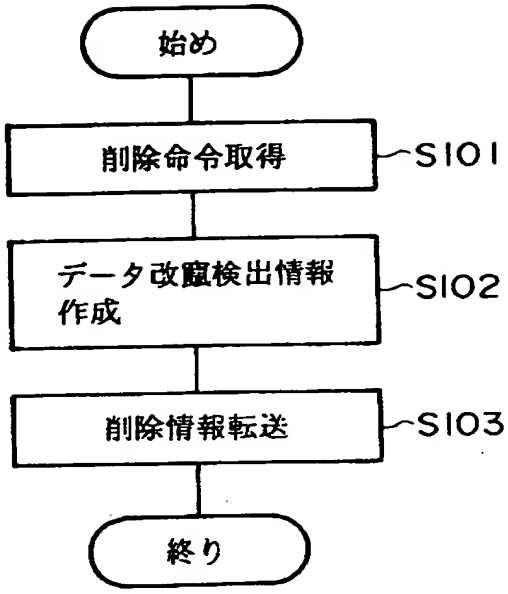
【図８】


始め
暗号化共通鍵Ｂ及び鍵情報取得
S801
暗号化共通鍵Ｂの復号化
S802
共通鍵改竄検出情報作成
S803
S804
共通鍵改竄検証
不正当
正当
暗号化共通鍵Ｃ作成
S805
暗号化共通鍵Ｃ転送
S806
終り

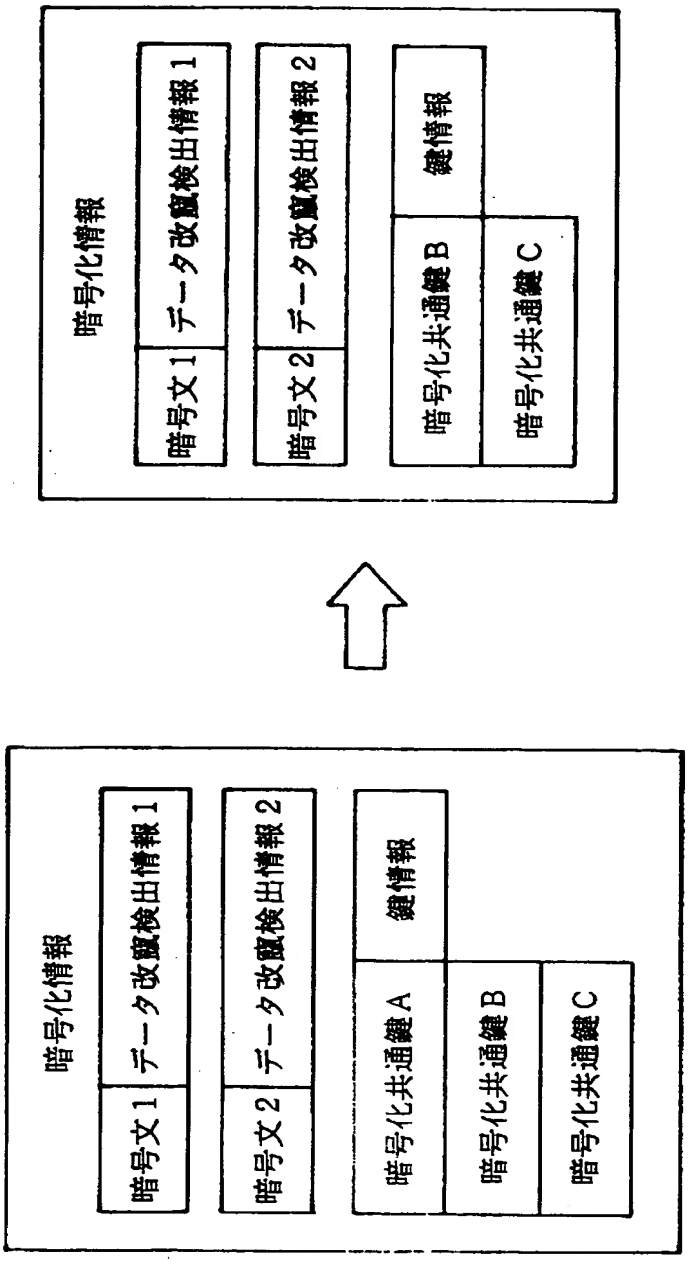
【図９】


暗号化情報
暗号文１
データ改竄検出情報１
暗号文２
データ改竄検出情報２
暗号化共通鍵Ａ
鍵情報
暗号化共通鍵Ｂ
暗号化共通鍵Ｃ
暗号化情報
暗号文１
データ改竄検出情報１
暗号文２
データ改竄検出情報２
暗号化共通鍵Ａ
鍵情報
暗号化共通鍵Ｂ

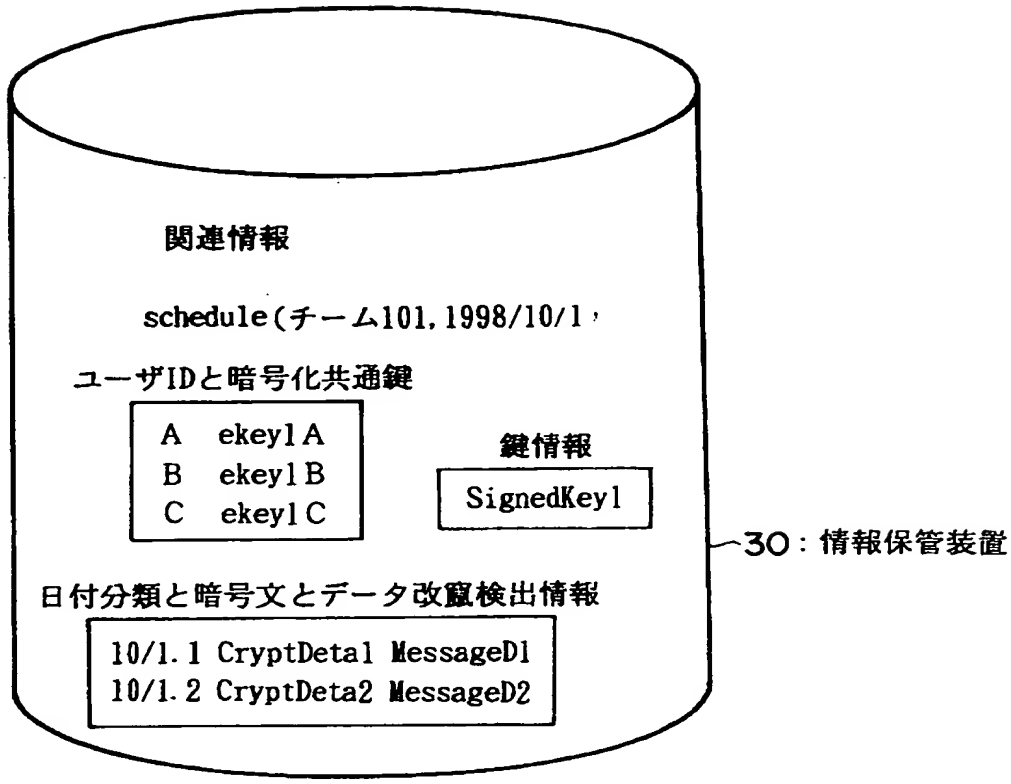
【図１０】



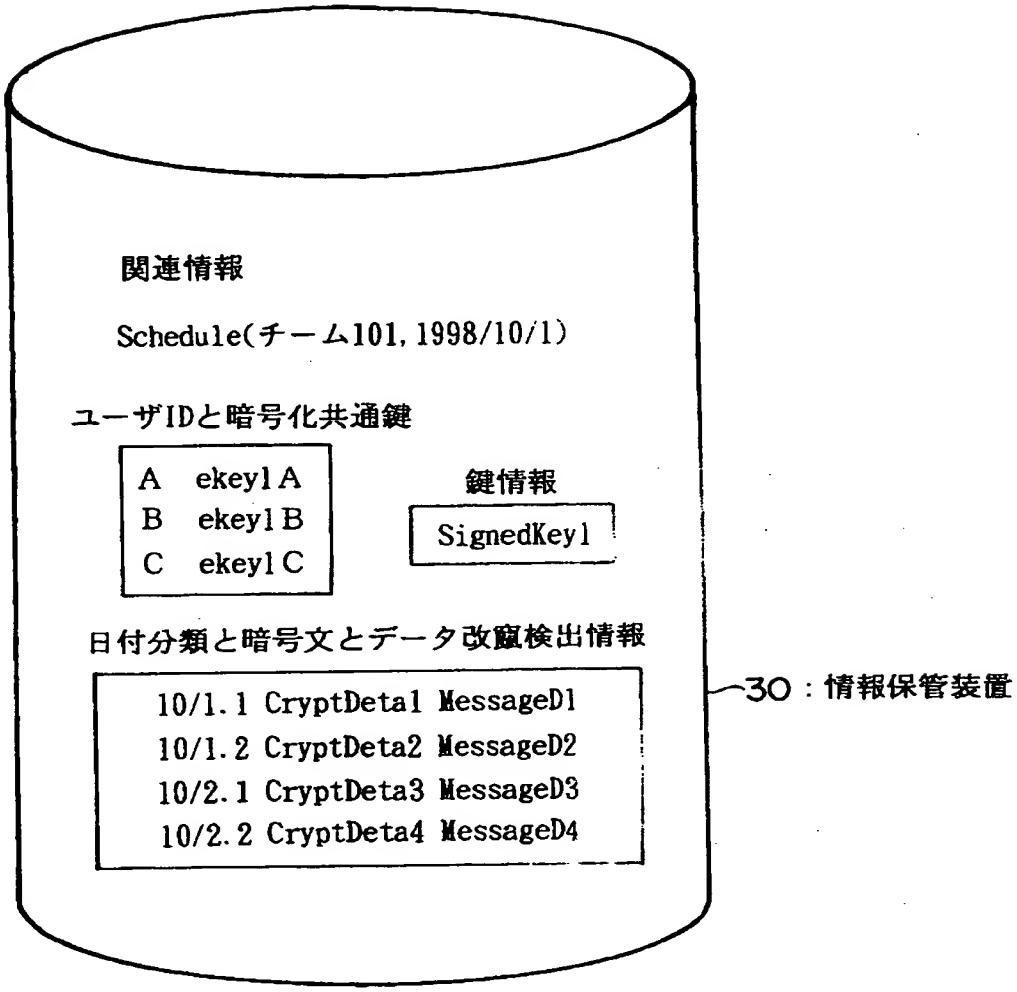
【図１１】


暗号化情報
暗号文１
データ改竄検出情報１
暗号文２
データ改竄検出情報２
暗号化共通鍵Ａ
暗号化共通鍵Ｂ
鍵情報
暗号化情報
暗号文１
データ改竄検出情報１
暗号文２
データ改竄検出情報２
暗号化共通鍵Ｂ
暗号化共通鍵Ｃ
鍵情報

【図１２】


関連情報
schedule(チーム101,1998/10/1,
ユーザIDと暗号化共通鍵
A ekey1A
B ekey1B
C ekey1C
鍵情報
SignedKey1
30：情報保管装置
日付分類と暗号文とデータ改竄検出情報
10/1.1 CryptDeta1 MessageD1
10/1.2 CryptDeta2 MessageD2

【図１３】


関連情報
Schedule(チーム101,1998/10/1)
ユーザIDと暗号化共通鍵
A ekey1A
B ekey1B
C ekey1C
鍵情報
SignedKey1
日付分類と暗号文とデータ改竄検出情報
10/1.1 CryptDeta1 MessageD1
10/1.2 CryptDeta2 MessageD2
10/2.1 CryptDeta3 MessageD3
10/2.2 CryptDeta4 MessageD4
30：情報保管装置

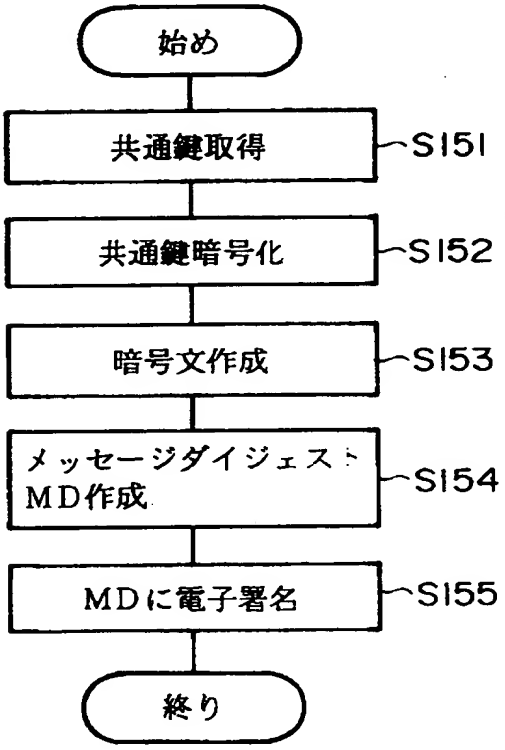
【図１４】

チーム１０１：スケジュール

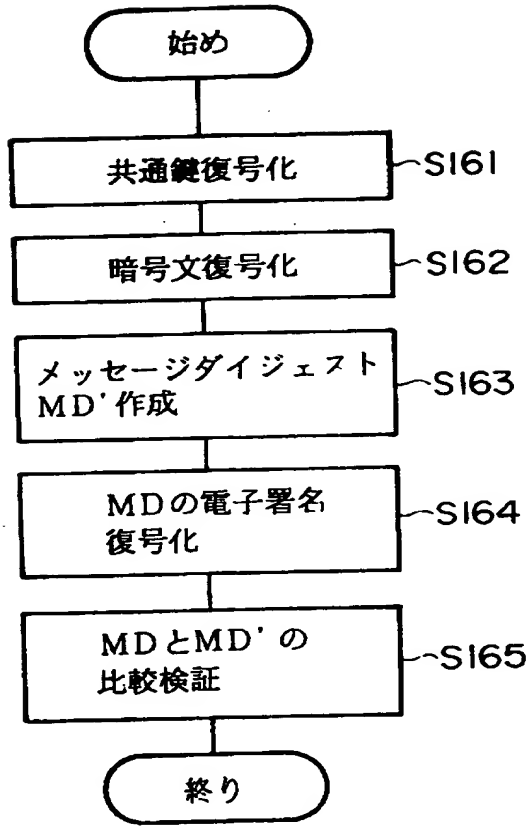
１０月

１日 B：セミナー参加 15:00～	２日 A:会議 17:00～	

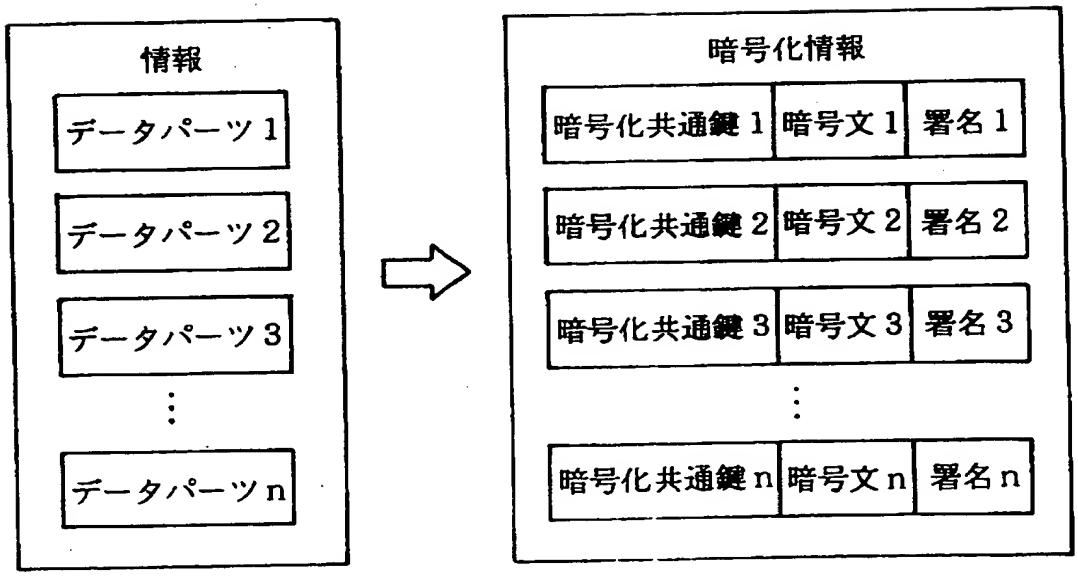
【図１５】



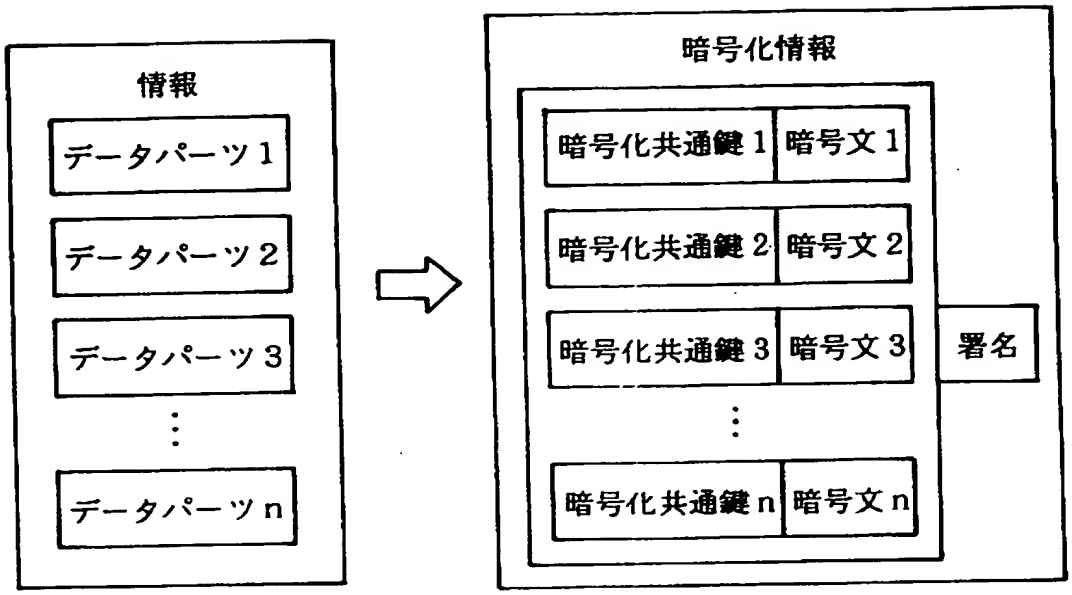
【図１６】


始め
共通鍵復号化
S161
暗号文復号化
S162
メッセージダイジェスト
MD'作成
S163
MDの電子署名
復号化
S164
MDとMD'の
比較検証
S165
終り

【図１７】


情報
データパーツ１
データパーツ２
データパーツ３
データパーツｎ
暗号化情報
暗号化共通鍵１
暗号文１
署名１
暗号化共通鍵２
暗号文２
署名２
暗号化共通鍵３
暗号文３
署名３
暗号化共通鍵ｎ
暗号文ｎ
署名ｎ

【図１８】


情報
データパーツ１
データパーツ２
データパーツ３
データパーツｎ
暗号化情報
暗号化共通鍵１
暗号文１
暗号化共通鍵２
暗号文２
暗号化共通鍵３
暗号文３
暗号化共通鍵ｎ
暗号文ｎ
署名

【書類名】　　要約書

【要約】

【課題】　複数の共有メンバーからなるチームで暗号化情報を共有可能とし、暗号化情報自体のオーバーヘッドが少なく、また改竄検証を可能とする暗号化復号化装置を提供する。

【解決手段】　本発明の暗号化復号化装置は、暗号化に際し、平文の暗号化・復号化に共通鍵方式を用い、各暗号文ごとに第１改竄検出情報を作成し、共通鍵を共有メンバー毎の公開鍵で暗号化するとともに共通鍵の改竄を検出するための鍵情報を１つのみ作成する。また復号化に際しては、復号化した共通鍵から共通鍵改竄検出情報を作成し、鍵情報と比較し共通鍵の改竄を検証する。また復号化した平文から第２改竄検出情報を作成し、第１改竄検出情報と比較し平文の改竄を検証する。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
　【識別番号】　000006264
　【住所又は居所】　東京都千代田区大手町１丁目５番１号
　【氏名又は名称】　三菱マテリアル株式会社
【代理人】　申請人
　【識別番号】　100064908
　【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
　【氏名又は名称】　志賀　正武
【選任した代理人】
　【識別番号】　100108578
　【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
　【氏名又は名称】　髙橋　詔男
【選任した代理人】
　【識別番号】　100089037
　【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
　【氏名又は名称】　渡邊　隆
【選任した代理人】
　【識別番号】　100101465
　【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
　【氏名又は名称】　青山　正和
【選任した代理人】
　【識別番号】　100094400
　【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
　【氏名又は名称】　鈴木　三義
【選任した代理人】
　【識別番号】　100106493
　【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
　【氏名又は名称】　松冨　豊
【選任した代理人】

【識別番号】　100107836
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　西　和哉
【選任した代理人】
【識別番号】　100108394
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　今村　健一
【選任した代理人】
【識別番号】　100108453
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　村山　靖彦
【選任した代理人】
【識別番号】　100100077
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　大場　充

出　願　人　履　歴　情　報

識別番号　　〔０００００６２６４〕

１．変更年月日　　１９９２年　４月１０日
［変更理由］　住所変更
住　所　　東京都千代田区大手町１丁目５番１号
氏　名　　三菱マテリアル株式会社